ABSTRACT

The invention relates to the protection of cryptographic methods against DPA-type covert channel attacks and, in particular, to a cryptographic method during which an x^d-type modular exponentiation is performed, wherein d is a whole number exponent of m+1 bits. The method includes scanning the d bits from left to right in a loop subscripted by i varying between m and 0; and, with each revolution of rank i, calculating and saving an updated partial result equal to x^b(i) in an accumulator (R0), b(i) being the most significant m-i+1 bits of exponent d (b (i)=$d_{m>i}$). According to the invention, at the end of a revolution of randomly-selected rank i(j) (i = i(0)), a randomization step E1 is performed, in which a random number z (z= b(i(j)), z = b (i(j)) $.2^t$, z = u) is subtracted from part of the d bits that have not yet been used ($d_{i-1->0}$) in the method. Subsequently, once the d bits modified by randomization step E1 have been used, a consolidation step E2 is performed, which involves saving (R0 <- R1xR0), in the accumulator (R0), the result of the multiplication of the contents of the accumulator (x^b(i)) by a number that is a function of x^z stored in a register (R1).